Ducera Securities LLC - Anti-Money Laundering Policy

In accordance with FINRA Rule 3310, and in an effort to comply with the applicable requirements under the USA PATRIOT Act and the Bank Secrecy Act, the Company has established the following policies and procedures for the purpose of attempting to deter and detect money laundering activities by customers. All employees and associated persons of the Company must comply with the applicable provisions under the Bank Secrecy Act and the AML provisions under the USA PATRIOT Act and every employee and associated person of the Company is expected to be familiar with the policies and procedures herein and to make reasonable efforts to comply with them. Failure to do so will result in disciplinary action and possible subsequent termination of employment. Company personnel, in following the enclosed policies, will also assist in detecting and deterring check fraud, ID theft, embezzlement, securities fraud, insider trading and other illegal activities not strictly related to money laundering.

1.1 Commitment Statement

The Company and its associated persons are strongly committed to cooperating with all applicable rules and regulations designed to combat money laundering activity. It is the responsibility of all persons associated with the Company to make every effort to protect the Company from exploitation by money launderers and to comply with applicable laws, regulations and Company policies in this regard.

1.2 Attestation

Each associated person by virtue of their association with the Company agrees to abide by Company's policies and procedures at set forth herein.

1.3 Designated Personnel

The Company has designated an Anti-Money Laundering Compliance Officer, who is identified in in Appendix A of this Manual, and herein known as "AMLCO".

The AMLCO will:

- Be responsible for implementing and monitoring the day-to-day operations and internal controls of the program;
- Act as the contact point for all employees and associated persons who have suspicions or concerns and all personnel are encouraged to consult the AMLCO for guidance;
- Serve as the initial point of authority in the process of determining whether or not certain unusual activities constitute reportable suspicious activities;
- Monitor applicable changes to the Bank Secrecy Act and USA PATRIOT Act, the regulations thereunder, and update the Company's procedures to comply with such changes;
- Inform the Company's designated Principal responsible for associated person education and training of changes in applicable laws and regulations; and
- Act as the central point of contact for communicating with regulatory agencies regarding money laundering issues.

Designated Principals as identified in Appendix B of the Company's WSP will assist the AMLCO in implementing and monitoring these procedures. These designated Principals may also act as

sounding boards for associated persons who detect potential suspicious activities and will ensure internal reporting of such suspicions to the AMLCO, when appropriate.

The CCO will assist the AMLCO in creating or amending procedures as needed to address changes to regulations and will provide guidance and support to the AMLCO in the reviewing and reporting of suspicious activities if requested.

1.4 FINRA Contact System

So that the Company can promptly receive alerts from FinCEN and other entities, within 17 business days after the end of each calendar year, the Super Account Administrator ("SAA') will review and update, if necessary, the information relevant to the Company's AML contact(s). If the AMLCO, or others receiving FinCEN 314a notices, changes during the year, the AMLCO must update the Company's contact information promptly through the FINRA Contact System to ensure that notices from FinCEN are received in a timely manner by the appropriate party.

1.5 Preliminary Risk Assessment

The purpose of the preliminary risk assessment is to determine, given the types of products or transactions in which the Company operates, the likelihood of suspicious or potentially illegal activity. Associated persons are required to consider the following factors when opening new accounts or reviewing the activities of existing accounts:

- Whether the customer is an individual, an intermediary, a public, private, domestic or foreign corporation, a financial or non-financial institution, or a regulated person or entity;
- Whether the customer has been an existing customer for a significant period of time;
- How the customer became a customer of the Company;
- Whether the business of the customer, or the particular type of account, is the type more likely to be involved in illicit activity (e.g., cash intensive business);
- Whether the customer's home country is a member of the Financial Action Task Force (FATF) or is otherwise subject to adequate anti-money laundering controls in its home jurisdiction; and
- Whether the customer resides in, is incorporated in or operates from a jurisdiction with bank secrecy laws, or one that has otherwise been identified by a regulatory or law enforcement agency or the Company as an area worthy of enhanced scrutiny.

In reviewing other risk factors or performing due diligence of persons or entities located outside the US, an associated person must consider the location of the potential customer to determine whether the location could increase any potential risk as well as the business purpose of the entity, source of funds and beneficial owners, where applicable.

Associated persons must attempt to evaluate the risk of each new customer, based on factors outlined above, and if heightened risk is perceived, bring such concerns to the attention of their designated supervisor. The supervisor shall evaluate the facts prior to the person becoming a customer and will adopt special monitoring procedures, if necessary, based on the risk. The information used in evaluating risk as well as developing any heightened monitoring procedures will be outlined in the customer file and documented during reviews of applicable activities. If the supervisor has questions relative to the perceived risk, they shall consult with the AMLCO, who shall make a final determination on the risk profile of the customer.

1.6 Definition of a Customer and Account

For purposes of evaluating risk, the associated must also consider whether or not the person is a customer as defined by applicable AML rules and regulations. Under the Bank Secrecy Act, the terms "customers" and "accounts" are defined as follows:

Customer (or "client" as used herein) refers to a person who opens a new account for an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person.

The following persons are excluded from the definition of customer:

- Persons completing new account documentation for another person, who are not also party to the account;
- Persons with trading authority over accounts (unless necessary to verify the customer's identity): and
- Existing customers, provided the Company has a reasonable belief that it knows the true identity of such person.

The following entities are also excluded from the definition of customer:

- A financial institution regulated by a federal functional regulator, such as:
  - The Board of Governors of the Federal Reserve;
  - Federal Deposit Insurance Corporation;
  - National Credit Union Administration;
  - Office of the Comptroller of the Currency;
  - Office of Thrift Supervision;
  - Securities and Exchange Commission; or
  - Commodity Futures Trading Commission) or a bank regulated by a state bank regulator.
- A department or agency of the United States, any State, or any political subdivision of any State;
- Any entity, other than a bank, whose common stock or analogous equity interests are listed on the NYSE Euronext or, AMEX, the separate "NASDAQ Small-Cap Issues" (now known as NASDAQ Capital Markets) heading; and
- Any entity established under the laws of the United States, of any state, or of any political subdivisions of a State that exercises governmental authority on behalf of the United States, any State, or any political subdivision of a State.

Account refers to a formal relationship with the Company established to effect transactions in securities. For purposes of this Manual, "account" shall be used to describe any formal relationship with a customer.

The following are excluded from the definition of account:

- An account that the Company acquires through any acquisition, merger, purchase of assets, or assumption of liabilities; and
- An account opened for the purpose of participating in an employee benefit plan established under ERISA.

Associated persons should consult their supervisor, the AMLCO, or the CCO if uncertain whether a person should be treated as a customer.

1.7 Customer Identification Program – Customers

The Company may do business with entities excluded from the definition of customer, as outlined above, in addition to individuals and entities not excluded from the definition of customer. The Company has determined that it will follow the procedures contained herein relative to identifying and verifying the identity of all individuals and entities with whom it will do business.

1.8 Customer Identification Program – Customer Notification

Customers must be provided with adequate notice that the Company is requesting information to verify their identities. The Company must provide the notice in a manner reasonably designed to ensure that a customer is either able to view the notice, or is given notice, before opening an account.

The Company requires Registered Representatives to orally provide notification to each customer prior to opening an account or establishing a relationship and to record in the customer documentation when notice was provided and to whom. The designated Principal in his review of customer information will ensure that the required notice is being delivered prior to the account or the relationship being opened.

1.9 Customer Identification Program – Necessary Customer Information

The Company requires its Registered Representatives to obtain the following information for each new customer:

- Name of the person(s) or entity;
- Date of birth for an individual;
- An address, which will be:
    - for an individual, a residential or business street address, or if neither exists, an Army Post Office or Fleet Post Office box number, or the residential or business street address of next of kin or another contact individual; or
    - for an account other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location;
    - for an individual in a state address confidentiality program, the street address of the ACP sponsoring state agency, since the person in the program is treated as not having a residential address and the agency sponsoring the ACP or another state agency is considered as another contact person for these individuals, and
- An identification number, which will be:
    - for a U.S. person, a taxpayer ID number; or
    - for a non-US. person, one or more of the following:
        - a taxpayer ID number;
        - a passport number and country of issuance;
        - an alien identification card number; or
        - the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

For a foreign business that does not have an identification number, the Company will request and maintain alternative government-issued documentation confirming the existence of the business.

If a customer has applied for, but has not received, a taxpayer ID number, the Registered Representative should alert his or her supervisor, who will determine whether or not proposed engagement or account opening may continue with the available information. If the supervisor permits the engagement or account to be opened without the TIN, the Registered Representative will be required to make efforts to obtain the TIN number by contacting the customer on or about the estimated receipt date and frequently thereafter, if necessary. All attempts to receive the number must be noted in the customer file. Without acceptable reasons for any delay, if the Company has not received the TIN within 60 days after the estimated receipt date, the account must be closed or engagement terminated (unless the AMLCO extends this deadline).

If a new or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Registered Representative must immediately notify his or supervisor who will review the facts and circumstances. If the supervisor finds that the customer intentionally provided false or misleading documents or information or will not respond to the supervisor's request, the Company will not open a new account or engagement. For an existing customer, after considering the risks involved, the supervisor will consult with the AMLCO and CCO to determine if the Company should closing any existing account or engagement.

In either case, the AMLCO must be notified immediately to determine whether or not to report the situation to FinCEN on a FinCEN SAR as described in the procedures relative to Official Reporting below.

1.10 Customer Identification Program – Verification of Identity

The Company's goal is to know, based on a reasonable belief, the true identity of its customers. Toward that goal, Registered Representatives are required to attempt to verify each customer's identity prior to opening an account or relationship and to document such verification efforts. During this process, Registered Representatives and other Company personnel are expected to note and analyze any logical inconsistencies in the information obtained.

Registered Representative are expected to use documentary means in verification efforts, where available. Possible sources of documentary verification include:

- For an individual, an unexpired government-issued identification evidencing nationality or residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; or
- For a customer other than an individual, documents showing the existence of the entity; the identity of its officers, partners, members, trustees or beneficiaries, as applicable; and the identity of persons authorized to act on its behalf, such as certified articles of incorporation, a government-issued business license, an operating agreement or by-laws, a partnership agreement, or a trust agreement.

The Company is not required to maintain copies of the documents containing personal information, such as a driver's license, passport or similar documents because of privacy concerns. However, the Registered Representative must record the type of document reviewed, the issuer of the document (i.e. state or country), the identification number and the expiration date.

Registered Representatives are not expected to determine whether such documents are valid; however, if some obvious form of fraud is evident, such as the document being tampered with or altered, Registered Representatives should not accept the document as verification and should

consult the AMLCO for assistance and further investigation. If the verification document is merely expired or damaged, but does not appear to be tampered with, then the Registered Representative should attempt to verify through another document or through non-documentary means.

When documentary verification methods are not available or practical or instances where the materials presented are not sufficient to meet the requirements as documentary evidence, a Registered Representative should consult his or her supervisor to discuss the circumstances and to determine the best method of non-documentary means of verification to employ.

Non-documentary methods of verifying identity include:

- Contacting a customer at his residence or place of business;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions;
- Obtaining a financial statement; or
- Any other reasonable means of attempting to verify the customer's identity, such as testing phone numbers or e-mail addresses provided.

In cases where non-documentary verification is used, the Company must retain a copy of the information gathered. The documentation may include notes regarding contacts with the customer or references, copies of financial statements or reports from consumer reporting agencies. Where a web search is used to verify identity or information provided by the customer, the Company should utilize information from a source other than one created by the customer in its verification efforts and should maintain a copy of the web pages reviewed as evidence of verification.

If the Registered Representative cannot obtain sufficient information to verify the identity of a new customer, they must immediately notify the supervisor and the AMLCO who will review the facts, circumstances and potential risk of doing business with the customer while such information is pending.

If the supervisor and AMLCO determine that the risk is high and cannot be adequately managed through restricting activities, heightened surveillance, internal controls, or any combination thereof, then the account or relationship will not be opened and the supervisor will notify the customer. Documentation regarding the review and notification will be maintained in the Company's AML files.

If the supervisor and the AMLCO determine that the risk is manageable through restricting activities, heightened surveillance, internal controls, or any combination thereof, while additional verification attempts are being made, the AMLCO will issue the restrictions in writing to the supervisor who will inform the Registered Representative and the customer. A copy of the restrictions will be retained in the customer file. Once sufficient information has been made, the AMLCO and supervisor will determine if the restrictions may be lifted and will notify the Registered Representative and customer of their decision. The supervisor, during reviews of customer activity, will ensure that these restrictions are followed. If violations of the restrictions are detected, the account or relationship will be immediately terminated.

If the supervisor and the AMLCO determine that the risk is low because the customer was referred by an existing customer, is known to one of the Principals of the Company or for another reason,

they will document their determination and advise the Registered Representative that the account or relationship can be opened. Copies of the review and determination will be maintained in the customer file.

During regular reviews, the supervisor shall verify that information sufficient to form a reasonable belief as to the identity of the customer is being retained in the customer's file.

1.11 Customer Identification Program – Additional Due Diligence

The Company recognizes that the risk of not knowing the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust created or conducting substantial business in a jurisdiction designated as a primary money laundering jurisdiction, a terrorist concern, or designated as a non-cooperative country or territory. The Company will identify customers that pose a heightened risk of not being properly identified.

When the CCO, AMLCO, or a supervisor identifies a customer that presents such a heightened risk, the Registered Representative or the supervisor must take measures to obtain information about persons associated with the customer, such as:

- Persons with beneficial ownership; or
- Individuals with authority and control over the account.

Based on the specific circumstances and the risks of not knowing the true identity of the customer, the AMLCO will determine the nature and extent of the additional measures that will be taken in each instance. As an example, the AMLCO may determine that the Company should obtain the identifying information required for all customers and specific documentary or non-documentary verifying information.

Once enhanced due diligence is complete, the AMLCO in consultation with the supervisor and the CCO will determine if the account or relationship can be opened and, if so, any special conditions that will be placed around the business or monitoring of the account and activities.

The AMLCO must ensure that all information received is maintained in the customer's file, and remains confidential. This information, if indicative of suspicious activity, will be used in internal or official reporting, as described below.

1.12 Comparison to Government Lists and Requests from Authorities

9.12.1 FinCEN 314(a) Requests

Every other week, or more frequently when needed, FinCEN posts a list of persons and/or entities suspected of criminal activity through its secure website, on behalf of various law enforcement entities, for review by financial institutions. A notification relative to the postings is sent to the Company's AML contact person(s), as shown on the FINRA Contact System as well as to any persons registered directly with FinCEN to receive such notices.

The AMLCO is responsible for ensuring the information on these postings is checked against a listing of the Company's current customers and any customers with whom the Company has conducted business within the previous 12 months, or longer if set forth in the posting, to determine if any customer appears on the list (a "match"). This review

must be completed within 14 days, or by the due date in the posting, to ensure reporting of any matches within 14 days or the specified time frame in the posting.

1.12.1.1 FinCEN 314(a) Requests – Review and Reporting

If a potential match is found, the AMLCO will investigate the potential match to verify if it is a true match or a false positive. If the match is a false positive, the AMLCO will make a note in the Company's 314(a) Review file describing the review. If the match is found to be a true match, the AMLCO will record such in the Company's 314(a) Review file, notify senior management and respond to the FinCEN request indicating the positive hit within 2 weeks of the request being posted.

The requesting law enforcement agency will then follow-up directly with the Company. The AMLCO will be responsible for responding to any such inquiries.

1.12.1.2 FinCEN 314(a) Requests – Documentation

In lieu of a self-verification report, FinCEN now makes available an activity report that the Company can run to evidence their review of notifications. The AMLCO will ensure that the Company prints a copy of this report at least annually and maintains it in the AML 314a Review file. The AMLCO will also print the report upon request for required testing and regulatory examinations.

1.12.2 Office of Foreign Assets Control (OFAC)

OFAC rules are enforceable by the Departments of the Treasury's Office of Foreign Assets Control ("OFAC"). Under these rules, and a 2001 Executive Order targeting terrorists, the Company and its associated persons are prohibited from conducting business with any persons or entities identified as "Terrorists" or "Specially Designated Nationals and Blocked Persons," or in any embargoed countries or regions appearing in the lists published on OFAC's website ("OFAC List"). Lack of compliance with OFAC rules may result in civil or criminal penalties.

In order to ensure compliance with OFAC rules, the Company will review for all new customers against the OFAC list prior to engaging in new business with these persons or entities. In addition, the Company will screen customers, with whom there is an ongoing relationship, against the OFAC list at least annually.

During a search of the OFAC List, whether or not a match is found, the person conducting the review must print out the results. If no match is found, the reviewer will file the results in the customer file.

If a match is found, the person conducting the review of the OFAC List must print out the result and notify the AMLCO immediately. The AMLCO will conduct another search of the OFAC List to determine if it is a true match. If the match is false, the AMLCO will note the results of his review on the printout and retain it in the customer's file. In cases where questions remain after attempting to determine whether a match is a false positive, the AMLCO should contact OFAC for assistance.

If the match is found to be true, the AMLCO will advise the appropriate designated supervisor to reject the transaction and/or block the customer's assets. The AMLCO will file a blocked assets or rejected transaction form with OFAC within 10 days, as applicable, and will call the OFAC Hotline at (800) 540-6322 immediately. In cases where the Company maintains accounts or assets which have been blocked, the AMLCO will file a report with OFAC annually. Any filings, such as the blocked assets forms and rejected transaction forms, will be retained in the Company's AML files.

If a search results in the customer's country being identified as under "limited" sanctions, the Company may continue without reporting to OFAC.

The designated Principal will verify that an OFAC List check has been completed and there is evidence of the results of the review in the customer file during the review and approval of new customers. If the OFAC List check has not been done or documentation as to the results are not present, the designated Principal will discuss the matter with the Registered Representative, run an OFAC List check and place the results in the customer's file.

Evidence of ongoing OFAC reviews will be maintained in the Company's OFAC file, along with any documentation related to the reporting of positive or false positive matches.

1.12.3 Other Lists

Should the Company or AMLCO receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for customer identification program purposes, the AMLCO will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list and will follow all federal directives issued in connection with such lists.

A copy of any such lists and the results of the AMLCO review will be maintained in the Company's AML files.

1.12.4 Requests from Law Enforcement

Should the Company receive a written request from a federal law enforcement officer or others for information concerning an account or customer, suspicious activities or other matters, the AMLCO will verify that the request is legitimate and then will provide requested information to the requesting officer or agency by the due date stated in the request. The AMLCO shall ensure that all such requests are kept confidential.

1.13 Accounts Requiring Special Monitoring

In addition to special monitoring conducted on accounts or relationships deemed high risk and subjected to such after the AMLCO's enhanced due diligence, certain accounts by their nature will require enhanced review upon opening and through the life cycle of the account or relationship.

1.13.1 Correspondent Accounts of Foreign Financial Institutions

Correspondent accounts of foreign financial institutions include any account established for a foreign financial institution to receive deposits from, or to make payments or other

disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution. This broad definition requires a formal relationship through which the financial institution provides regular services.

The Company does not open accounts. In the event a Representative has a question about a current or prospective customer or whether a current or prospective relationship may be a correspondent account for a foreign financial institution, they must immediately consult the AMLCO, who will investigate.

If the AMLCO determines a current or proposed relationship is not or will not be a correspondent account for a foreign financial institution, the AMLCO will so advise the Representative and any current relationship may be continued and any prospective relationship may be opened. If the AMLCO is not satisfied that such a correspondent relationship does not exist or would not be created, the AMLCO will require the termination of the existing relationship or deny the opening of the proposed relationship.

1.13.2 Private Banking Accounts of Non-US Persons or Entities

A "private banking" account is an account (or any combination of accounts) that requires a minimum aggregate deposit of $1,000,000, is established for one or more individuals and is assigned to or administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

The Company does not open accounts. In the event a Representative has a question about a current or prospective customer or whether a current or prospective relationship may be a private banking account, they must immediately consult the AMLCO, who will investigate.

If the AMLCO determines a current or proposed relationship is not or will not be a private banking account, the AMLCO will so advise the Representative and any current relationship may be continued and any prospective relationship may be opened. If the AMLCO is not satisfied that a private banking account does not exist or would not be created, the AMLCO will require the termination of the existing relationship or deny the opening of the proposed relationship.

1.13.3 Accounts of Senior Foreign Political Figures

A "senior foreign political figure" is a current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not the person is or was an elected official, a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise. This definition also includes a corporation, business, or other entity formed by or for the benefit of such an individual. Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources. Also included in the definition are immediate family members of such individuals, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure.

The Company does not open accounts. In the event, a representative has a question about whether or not a customer could be considered a senior foreign political figure, they must immediately consult the ALMCO, who will conduct an investigation and determine

whether or not there is a relationship to such an account. If the AMLCO determines the there is no relationship to a senior foreign political figure, he will advise the representative that the relationship may be opened. If the AMLCO still has questions regarding the customer or believes that the request is being made on behalf of a senior foreign political figure, the request will be denied and no relationship will be opened.

1.13.4 Accounts for Marijuana-Related Businesses

While some states have enacted laws making the medical and/or recreational use of marijuana legal within their jurisdictions, the use, production or distribution of marijuana is still illegal under federal law. Therefore, while financial services firms may open accounts for such businesses operating in states where the production, distribution, or use of marijuana is legal, they must do additional due diligence on these businesses to ensure they are licensed to operate within the state and are operating in accordance with their license. Further, financial institutions must monitor the activities of such businesses to ensure they continue to operate in accordance with state licensing requirements and guidance put forth by the Department of Justice in the "Cole Memo."

The Company does not permit the opening of accounts for marijuana-related businesses, its owners or employees. If the Representative or the designated Principal determines that an account has been opened for marijuana-related businesses, its owners or employees, the designated Principal must report such to the AMLCO and take steps necessary to immediately close the account.

1.13.5 Section 311 of the USA PATRIOT Act

Although the Company does not permit the opening of accounts of foreign institutions or those which engage in business in foreign jurisdictions, the AMLCO must review any rules promulgated under Section 311 and follow any prescriptions or prohibitions contained therein., if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern.

1.14 Reliance on another Financial Institution

The SEC has granted a limited exemption so that broker-dealers may rely on another financial institution to perform some or all of the functions required to identify customers. OFAC has not granted any exemptions that would allow the Company to rely on another person or entity to conduct these screenings on their behalf. Therefore, broker-dealers entering into agreements with outside entities, including their clearing firm, to perform OFAC checks should verify that the screenings are being conducted and are accurate as they may still be held liable for any discrepancies or missed findings.

The Company does not rely on any other financial institution to perform any duties with respect to the Company's customer identification program or other areas of its Anti-Money Laundering Program.

1.15 Suspicious Activity Monitoring

1.15.1 Account and Relationship Opening

Registered Representatives and their designated Principals, in the process of gathering customer information and researching the subjects addressed above, must remain alert and aware of their prospective customers' actions and attitudes throughout the process. While suspicious activity may normally occur in the course of servicing existing accounts, certain actions by a prospective customer during the account opening stage may be indicators of money laundering intentions ("red flags"). By being perceptive, Registered Representatives will have the opportunity to take note of such red flags, which may include:

- A customer is reluctant to provide full details with respect to his or her identity, type of business or assets, or business activities, or furnishes unusual or suspect identification or business documents;
- A customer wishes to engage in transactions that lack business sense, apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy;
- A customer wishes to impose requirements inconsistent with the Company's business or which could be more easily serviced elsewhere;
- A customer or person associated with the customer has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations;
- The firm experiences unusual difficulties and delays in obtaining copies of documentation related to incorporation or authorization;
- The firm finds that the customer, which is an LLC, has an address listed as the address of several other LLCs;
- The customer's actual business activities are inconsistent with the description of its business activities listed in its formation documents;
- A customer demonstrates ignorance of expectations regarding AML regulations and unreasonably denies requests for assurances relating to its own internal customer acceptance and AML policies and procedures; and
- A customer appears to be acting as the agent for another entity but declines, evades or is reluctant, without legitimate reasons, to provide any information in response to questions about that entity.

Any such behavior noted in the account opening stage must be noted in writing by the associated person and brought to the attention of the AMLCO. The AMLCO will review the facts and circumstances to determine if the account may be opened, if enhanced due diligence is required, or if suspicious activity reporting is required. The AMLCO will notify the Registered Representative and the designated Principal regarding the results of his review. If the AMLCO determines the account may be opened, documentation on the suspicions and the AMLCO's review will be maintained in the customer's file for future review. If the AMLCO determines that the account may not be opened, documentation will be maintained in the Company's Suspicious Activity file or FinCEN SAR file, as applicable.

1.15.2 Ongoing Monitoring

The Company's business does not involve the opening of an account or an ongoing relationship with the issuer/offeror or investor/buyer. Further, the Company does not maintain a record of an investor or buyer's investment holdings or any future transactions

with regard to an investment or purchase once a transaction has been closed. Therefore, the Company has no means to monitor ongoing activities.

If the Company is engaged by the same issuer/offeror for future business or introduces an investor/buyer to another issuer/offeror contracted by the Company, the AMLCO will review the new activities to determine if any could be considered suspicious and will document any suspicious activities in the Company's files.

1.16 Specific Activity Monitoring

1.16.1 Wire Transfers

Often referred to as the "Travel" rule, 31 CFR Section 1010.410(f) has been issued by FinCEN to help law enforcement agencies detect, investigate, and prosecute money laundering and other financial crimes by preserving an information trail about persons sending and receiving funds through funds transfer systems. This rule requires all financial institutions to pass on certain information to the next financial institution in certain funds transmittals involving more than one financial institution.

Entities transmitting funds equal to or greater than US$3,000 (or its foreign equivalent) are required to maintain records of a transmittal order for a period of 5 years including the name, address and account number of the transmitter; the identity of transmitter's financial institution; the amount of the transmittal order; the execution date of order; the identity of the recipient's financial institution and, if received, the name, address and account number of recipient and any other specific identifier.

The Company does not send or facilitate the sending of wire transfers for its customers. Should the Company's business change, the AMLCO will ensure that the Company has procedures in place to comply with the "Travel Rule."

1.16.2 Receipt of Cash or Currency

The Company does not accept cash or currency from customers. If a customer attempts to deposit cash or currency, or use cash or currency to pay for an investment or purchase, the funds shall not be accepted and the AMLCO must be notified immediately. If the Company changes its business the AMLCO will ensure that procedures relative to the receipt of cash or currency are implemented.

1.16.3 Receipt of Cash Equivalents or Checks

The Company does not accept checks or cash equivalents, including money order, cashier's checks or traveler's checks from customers as payment to settle securities transactions, unless the instrument is payable to the issuer/offeror, product sponsors/distributors, clearing firm or the escrow agent, as applicable, and they will accept the instrument. The associated person receiving the instrument must enter such on the Checks Received and Delivered blotter prior to forwarding it to the payee. If the payee will not accept the instrument the check will be returned to the investor/buyer with instruction on acceptable methods to remit payment.

Should the Company receive any such instruments payable to the Company, the associated person receiving the instruments must record them on the Checks Received and Delivered

blotter before returning the instruments with instructions on proper funds remittal to the investor/buyer.

The designated Principal will review the blotter monthly and evidence his review by initialing and dating the blotter.

1.16.4 Foreign Currency Transactions

The Company does not accept any cash payments in foreign currency or from foreign transactions for securities purchases. Should a customer attempt to make such a payment, the attempt should be rejected, notes of the attempt should be kept and the AMLCO should be notified.

1.16.5 Receipt of Securities

The Company does not accept securities from customers. If a customer sends securities to the Company for deposit into their account or in settlement of a transaction, the associated person receiving the certificates must log them on the Securities Received and Delivered blotter before returning the certificates to the customer with information on how to send them to the clearing firm or the transfer agent, as applicable. If the Company changes it business the CCO will ensure that procedures relative to the receipt of securities are implemented.

1.17 Suspicious Activity Reporting

The U.S. Department of the Treasury requires broker-dealers to report any questionable transaction or series of transactions in excess of US $5,000; however, voluntary reporting may take place for smaller dollar amounts in question.

The AMLCO, once having determined to file a FinCEN SAR, must file electronically within 30 days of being aware of the suspicious activity. Registration and information for e-filing of FinCEN SARs is available at http://bsaefiling.fincen.treas.gov.

A copy of the form and confirmation page of the electronic filing and all supporting documentation must be retained for five years. Neither the Company nor its employees may notify any person involved in a reported transaction that the transaction has been reported on a FinCEN SAR.

The Company is not required to close accounts or cease doing business with a customer who is the subject of a filed FinCEN SAR. The CCO and AMLCO must use their discretion in these cases. If accounts are left open, the designated Principal must monitor account activity carefully, wait for a response from FinCEN or other authority and continue to file FinCEN SAR reports every 90 days if the activity continues.

In some cases, FinCEN or another law enforcement agency may request that the Company keep the account open so they can conduct ongoing surveillance. This request must be in writing and specify the duration of time the account is to remain open, not to exceed six months. If the agency wishes the account to remain open longer than six months, it must provide the Company with subsequent written requests. The Company should verify the identity of the individual and agency making the request prior to granting such a request. The Company may refuse to honor this request as ultimate responsibility for the decision to keep an account open, ongoing monitoring and ongoing FinCEN SAR report filing rests with the Company and its Principals.

In the event the Company receives a subpoena requesting a copy of the FinCEN SAR or related information, the request should be forwarded immediately to the AMLCO. The AMLCO must deny the subpoena request and inform FinCEN of any subpoena received.

NOTE: Privacy policies under Regulation S-P do not apply to information provided to FinCEN in a FinCEN SAR and the Company and its employees are protected from liability for such required disclosures.

1.17.1 Confidentiality

The Company must not divulge any information on a FinCEN SAR filing to any employee not directly involved with the filing or to any non-parent affiliate of the Company. In general, the Company and its employees are prohibited from disclosing FinCEN SAR's or the fact that they were filed, to anyone other than to law enforcement agencies or securities regulators.

However, information underlying the filing, not the filing itself, may be disclosed to entities affiliated with the Company or other entities with whom the Company has a relationship, such as a clearing Company, if a 314(b) notification has been file by the Company and the other entity.

1.17.2 Sharing FinCEN SAR Information with a Parent Entity

Suspicious activity reports may be shared with parent entities, both domestic and foreign, for the purpose of allowing the parent entities to discharge their oversight responsibilities with respect to enterprise-wide risk management and compliance with applicable laws and regulations.

In the event the Company shares a FinCEN SAR filing with a parent entity and the parent includes persons not registered with the Company, the AMLCO, working with senior management, will ensure that prior to sharing such information the parent entity has entered into a confidentiality agreement with the Company. The agreement must be in writing and specify that the parent entity must protect the confidentiality of the FinCEN SAR through appropriate internal controls.

If the recipient is a foreign parent entity, the agreement must also require that the parent not disclose further any FinCEN SAR, or the fact that such report has been filed. However, the foreign parent entity may disclose, without permission, underlying information (that is, information about the customer and transaction(s) reported) that does not explicitly reveal that a FinCEN SAR was filed and that it is not otherwise subject to disclosure restrictions.

1.18 Other Reporting

1.18.1 Report of Foreign Bank and Financial Accounts

If the Company holds, or has signature authority or other authority over, a financial account in a foreign country of more than $10,000, the Company must file a Report of Foreign Bank and Financial Accounts ("FBAR, Form 114") with FinCEN. An FBAR is not required to be filed electronically. The Company is not required to file an FBAR on behalf of customers, but should advise customers of their obligation to file, if applicable.

However, if the Company has discretionary or signature authority over a foreign account, the Company will have an independent filing obligation.

1.18.2 State Reporting

Certain states require reporting to a state authority. The CCO, upon filing official forms with federal authorities, should make efforts to determine respective obligations of the states where the Company's office are located.

1.19 Information Sharing

The Company does not share information with other entities and does not maintain a clearing relationship. Therefore, no 314(b) certification filing has been made. Should the Company wish to share information with another entity or if they enter into a clearing relationship, the AMLCO shall ensure that the 314(b) filing is made prior to sharing any information or once the clearing arrangement is effective.

1.20 Recordkeeping

Records created as a result of compliance with this Anti-Money Laundering Compliance Program will include the following:

- Forms filed with federal and state authorities, such as FinCEN SAR, FinCEN CTR, FinCEN CMIR, FBAR; and any other forms required, such as the "Certification Regarding Correspondent Accounts For Foreign Banks";
- Internal reporting or review documents, including the Preliminary Suspicious Activity and P- SAR Review form;
- Notes, analyses and reflections of Company personnel, such as the Preliminary Risk Assessment, notes to account files and the results of monthly monitoring of specific activities, such as wire activity; and
- Results of independent testing for compliance with this Program (described below).

In accordance with applicable rules, the Company will create and maintain FinCEN SARs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification and funds transfers and transmittals, as well as any records related to customers listed on the OFAC list. The Company shall maintain all FinCEN filings and documentation related to FinCEN SAR filings for a period of no less than 5 years.

The Company will maintain will retain all other documents related to their AML program according to BSA rules and other record keeping requirements, including SEA Rules 17a-3 and 17a-4, as applicable.

All FinCEN SAR's filed with authorities must be maintained in the confidential records of the AMLCO, separate from the other books and records of the Company. The AMLCO and CCO are responsible for ensuring compliance with these record keeping policies.

1.21 Independent Testing

The purpose of the testing is to assess the adequacy of the written program and to assess the Company's degree of compliance with its AML procedures and should:

- Confirm the integrity and accuracy of the procedures for the reporting of large currency transactions;
- Include a review of FinCEN and other BSA forms filed with authorities;
- confirm the integrity and accuracy of the Company's record keeping activities and adherence to in-house record retention policies;
- Confirm compliance with the Company's "know your customer" policies by conducting a review of a sampling of new account documentation, account reviews and transaction reviews;
- Review the AMLCO's records as they relate to specific monitoring of transactions or accounts, or follow-up on reported unusual activity;
- Confirm adherence to the Company's internal reporting procedures;
- Confirm that all employees have been made aware of the Program, and have signed any attestations required by the Company;
- Include steps necessary to ascertain that the Company is conducting an ongoing training program; and
- Confirm that the Company's Anti-Money Laundering Compliance Program incorporates changes required as a result of new legislation or regulation.

1.21.1 Frequency of Testing

The AMLCO has reviewed the requirements under FINRA Rule 3310 and the BSA. Based on his review of the requirements, the Company's business and its customers, the AMLCO has determined that the Company's AML Program shall be tested every other calendar year.

If the Company's business or applicable rules change, or if advised by a regulator that annual testing is required, the AMLCO will amend the procedures accordingly.

1.21.2 Appointed Testing Personnel

The Company utilizes an outside service provider to conduct required independent testing of its AML Program and this party is identified in Appendix D of this Manual. The AMLCO has reviewed this party's qualifications and has determined that they are independent and qualified to conduct testing, as required under FINRA Rule 3310. The information reviewed in evaluating the provider's qualification and a copy of the contract/engagement agreement for the test are retained in the Company's AML testing file for the applicable year of the test.

1.21.3 Reporting

The AMLCO must present all reports relative to the results of the independent testing to senior management to alert them to any deficiencies in the Company's AML Program and allow the Company to take corrective and/or disciplinary action, as each situation warrants. The AMLCO must ensure that corrective action is taken when necessary and that copies of all reports of findings and documentation related to actions taken to remediate findings are maintained for a period of no less than five years in the Company's AML Testing file.

1.22 Training

The Company has appointed the AMLCO, in conjunction with the Continuing Education Principal, to provide AML training to all associated persons who play a role, or could play a role, in the identification and prevention of money laundering. The designated Principals and the AMLCO will review a record of associated persons annually and determine if based on their role or activities they would require training in AML related matters. The AMLCO will maintain a record of all personnel requiring training and will work with supervisory personnel and the Continuing Education Principal to determine the most appropriate training for each required person.

Training will be provided at least annually and training will be required for all new employees in covered roles and for all Registered Representatives. The Continuing Education Principal will be responsible for ensuring that required personnel complete their training and will notify the AMLCO and supervisor if someone fails to complete. A record of assigned training required to be completed by each required person or role and evidence of completion will be maintained in the Company's AML Training file.